8/05/2007

caGrid LOA1 Certificate Authority

Certificate Policy and Practice Statement

caGrid LOA1 Certificate Authority

Certificate Policy and Practice Statement

Table of Contents

Introduction 8

Overview 8

Registration Authorities 9
Account/Certificate Creation 10
Grid Proxy Certificate Creation 10
Host Certificate Creation 11

Document Name and Identification 11

PKI participants 11

Certification Authorities 11
Registration Authorities 11
Subscribers 12
Relying Parties 12
Other Participants 12

Certificate Usage 12

Appropriate Certificate Users 12
Prohibited Certificate Uses 12

Policy Administration 12

Organization Administering the Document 13
Contact Person 13
Person Determining CPS Suitability 13
CPS Approval Procedures 13

Definitions and Acronyms 13
Publication and Repository Responsibilities 16
Repositories 16
Publication of Certification Information 16
Time and Frequency of Publication 17
Access Controls on Repositories 17
Identification and Authentication 17
Naming 17
Types of Names 18
Need for Names to be Meaningful 19
Anonymity or Pseudonymity of Subscribers 19
Rules of Interpreting Various Name Forms 19
Uniqueness of Names 20
Recognition, Authentication, and the Role of Trademarks 20
Initial Identity Validation 20
Method to Prove Possession of Private Key 22
Authentication of Organizational Identity 22
Authentication of Individual Identity 22
Non-verified Subscriber Information 22
Validation of Authority 22
Criteria for Interoperation 23
Identification and Authentication for Re-key Requests 23
Identification and Authentication for routing Re-Key 23
Identification and Authentication for Re-key After Revocation 23
Identification and Authentication for Revocation Requests 23
Certificate Life-Cycle Operational Requirements 23
Certificate Application 23
Who can submit a certificate application 23

Enrollment Process and Responsibilities 24
Certificate and Application Processing 25
Performing Identification and Authentication Functions 25
Approval or Rejection of Certificate Applications 25
Time to Process Certificate Applications 25
Certificate Issuance 25
CA Actions during Certificate Issuance 25
Notification to Subscriber by the CA of Issuance of Certificate. 26
Certificate Acceptance 26
Conduct Constituting Certificate Acceptance 26
Publication of the Certificate by the CA 27
Notification of Certificate Issuance by the CA to Other Entities 27
Key Pair and Certificate Usage 27
Subscriber Private Key and Certificate Usage 27
Relying Party Public Key and Certificate Usage 27
Certificate Renewal 28
Certificate Re-Key 28
Certificate Modification 28
Certificate Revocation and Suspension 28
Facility, Management, and Operational Controls 29
Physical Controls 29
Site Location and Construction 29
Physical Access 29
Power and Air Conditioning 30
Water Exposure 30
Fire Prevention and Protection 30
Media Storage 31
Water Disposal 32
Off-site Backup 32

Procedural Controls 33

Personnel Controls 33

Audit Logging Procedures 33

Types of Events Recorded 33

Frequency of Processing Log 33

Retention Period for Audit Log 34

Protection of Audit Log 34

Audit Log Backup Procedures 34

Audit Collection System (internal vs external) 34

Notification of event-causing subject 34

Vulnerability Assessments 34

Records Archival 34

Key Changeover 34

Compromise and Disaster Recovery 34

Incident and Compromise Handling Procedures 35

Computing Resources, Software, and/or Data are Corrupted 35

Entity Private Key Compromise and Procedures 35

Business Continuity Capabilities after a Disaster 36

CA or RA Termination 36

Technical Security Controls 36

Key Pair Generation and Installation 36

Key Pair Generation 36

Private Key Delivery to Subscriber 36

Public Key Delivery to Subscriber 37

CA Public Key Delivery to Relying Parties 37

Key Sizes 37

Public Key Parameters Generation and Quality Checking 37

Key Usage Purposes (as per X.509 v3 key usage field) 37

Private Key Protection and Cryptographic Module Engineering Controls 37

Cryptographic Module Standards and Controls 37

Private Key (n out of m) Multi-Person Control 37
Private Key Escrow 38
Private Key Backup 38
Private Key Archival 38
Private Key Transfer into or from a Cryptographic Module 38
Private Key Storage on Cryptographic Module 38
Method of Activating Private Key 38
Method of Deactivating Private Key 38
Method of Destroying Private Key 38
Cryptographic Module Rating 38
Other Aspects of Key Pair Management 39
Public Key Archival 39
Certificate Operational Periods and Key Pair Usage 39
Activation Data 39
Computer Security Controls 39
Specific Computer Security Technical Requirements 39
Computer Security Rating 39
Life-Cycle Technical Controls 39
Network Security Controls 39
Time-Stamping 40
Certificate, CRL, and OCSP Profiles 40
Certificate Profile 40
Version Number(s) 40
Certificate Extensions 40
Algorithm Object Identifiers 40
Name Forms 41
Name Constraints 41
Certificate Policy Identifier 41
Usage of Policy Constraints Extension 41
Policy Qualifiers Syntax and Semantics 42

Processing Semantics for the Critical Certificate Policy Extension 42
CRL Profile 42
Version Numbers(s) 42
CRL and CRL Entry Extensions 42
OCSP Profile 42
Compliance Audit and Other Assessments 42
Other Business and Legal Matters 43
Fees 43
Financial responsibility 43
Confidentiality of Business Information 43
Intellectual Property Rights 43
Representations and Warranties 43
Disclaimers of Warranties 43
Limitations of Liability 44
Indemnification 44
Term and Termination 44
Term 44
Termination 44
Effect of Termination and Survival 44
Individual Notices and Communications with Participants 44
Amendments 44
Procedure for Amendment 44
Notification Mechanism and Period 45
Circumstances Under the OID Must be Changed 45
Dispute Resolution Provisions 45
Governing Law 45
Compliance and Applicable Law 45

- Miscellaneous Provisions 45
- Other Provisions 45

Document Source 45

Works Cited 46

Introduction

Overview

This Certificate Policy and Practice Statement (herein referred to as the ”Policy”) specifies minimum requirements for the issuance and management of digital certificates that will be used in authenticating users and services accessing the Cancer Biomedical Informatics Grid (caBIG™) resources and the resources of other entities (relying parties) that accept those certificates. The Policy is issued and administered under the authority of the National Cancer Institute Center for Biomedical Informatics and Information Technology (CBIIT). This document is structured according to Internet Engineering Task Force RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework). The caBIG Federation will adopt the e-Authentication standards as specified by The National Institute of Standards and Technology (NIST) Special Publication 800-63 Version 1.0.2 entitled *Electronic Authentication Guideline*. caBIG™ will operate certificate authorities(CA) in accordance with the Level of Assurance specified by NIST. This document specifies the policy for the operation of a LOA1 certificate authority, herein referred to as the caGrid LOA1 CA. The caGrid LOA1 CA consists of its own private key and certificate. It is expected that relying parties will trust the caGrid LOA1 CA, though a relying party may choose to trust other CA s as well. The caGrid LOA1 CA along with the associated software and repositories used to distribute policies, Certificate Revocation Lists (CRL) and the like are referred to as the “caGrid PKI” (Public Key Infrastructure).

This document covers the policy that applies to the caGrid LOA1 CA, which is operated and maintained by Dorian (1). Dorian is a grid service for the provisioning and management of grid users accounts. Dorian provides an integration point between external security domains and the grid, allowing accounts managed in external domains to be federated and managed in the grid. Figure 1 illustrates an example usage scenario for Dorian. To obtain grid credentials or a proxy certificate, users authenticate with their institution using the institution’s conventional mechanism. Upon successfully authenticating the user, the local institution issues a digitally signed Secure Access Markup Language (SAML) assertion, vouching that the user has authenticated. The user then sends this SAML assertion to Dorian in exchange for grid credentials. Dorian will only issue grid credentials to users that supply a SAML assertion from a *Trusted Registration Authority*. For example, in Figure 1 where a Georgetown user wishes to invoke a grid service that requires grid credentials, they first supply the application with their username and password to the Georgetown credential provider as they would normally do. The application client authenticates the Georgetown user with the Georgetown credential provider, receives a signed SAML assertion which it subsequently passes to Dorian in exchange for grid credentials. These credentials can then be used to invoke the grid services. This illustrates how Dorian can leverage an institution’s existing authentication mechanism and bring its users to the grid.

To facilitate smaller groups or institutions without an existing credential provider, Dorian also has its own internal credential provider (which is registered as a Trusted Registration Authority). This allows users to authenticate to Dorian directly, thereby enabling them to access the grid. The Dorian credential provider provides administrators with facilities for approving and managing users. All of the Dorian functionality is made available through a grid service interface. Figure 1 illustrates a scenario of a client using the Dorian IdP to authenticate to the Grid. In this scenario, the unaffiliated User wishes to invoke a grid service. Given that this unaffiliated user has registered and been approved for an account, she is able to authenticate with the Dorian IdP by supplying their username and password. Upon successfully authenticating the user, the Dorian IdP issues a SAML Assertion just like institutional IdPs, which can be presented to Dorian in exchange for grid credentials. The credentials can be used to invoke the grid service.

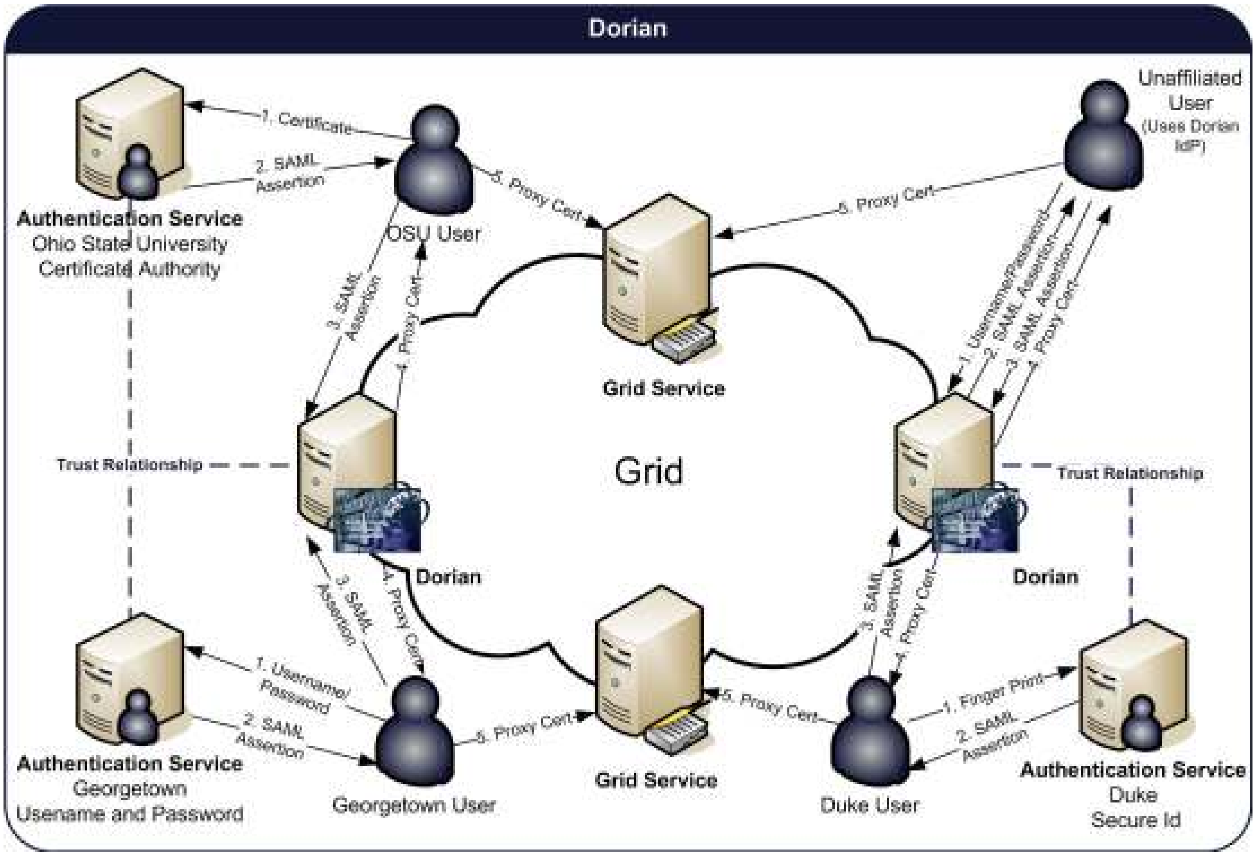

Dorian
1. Certificate
2. SAML Assertion
Authentication Service
Ohio State University
Certificate Authority
OSU User
5. Proxy Cert
Unaffiliated User
(Uses Dorian IdP)
5. Proxy Cert
3. SAML Assertion
4. Proxy Cert
1. Username/Password
2. SAML Assertion
3. SAML Assertion
4. Proxy Cert
Grid Service
Grid
Trust Relationship
Trust Relationship
Dorian
Dorian
3. SAML Assertion
4. Proxy Cert
3. SAML Assertion
4. Proxy Cert
1. Username/ Password
2. SAML Assertion
5. Proxy Cert
5. Proxy Cert
1. Finger Print
2. SAML Assertion
Authentication Service
Georgetown
Username and Password
Georgetown User
Grid Service
Duke User
Authentication Service
Duke
Secure Id

Figure 1 Dorian

Registration Authorities

The institutional credential providers that Dorian is configured to trust are referred to as Trusted Registration Authorities (RA). Dorian only creates credentials for users whose identity assertions are signed by a trusted registration authority. The set of trusted registration authorities can be managed by Dorian administrators through its grid service interface. The Dorian grid service interface provides functionality for adding, modifying, and removing Trusted Registration Authorities. The Trusted Registration Authorities information consists of the following: Id, Name, Status, User Policy, Certificate, and acceptable authentication methods. The Id is a unique id assigned by Dorian to identify the registration authority. The name is assigned by an administrator and provides human readable name to easily identify a registration authority. The Status specifies the current status of the registration authority: Active or Suspended. Users associated with a “suspended” registration authority will be refused access to Dorian and will be listed in the CRL of the Dorian CA. Each registration authority is associated with a set of configurable User Policies that are applied to each user when they authenticate. These policies designate how Dorian should handle users from a specified registration authority. As an example, a policy might dictate what to do when a new user tries to create grid credentials for the first time. An automatic approval policy would automatically register the user with Dorian and create a grid account for the user. A manual approval policy would automatically register the user but not enable the grid account until an administrator manually approves it. User policies can also be used to dictate what to do when a user's grid credentials expire. For example, an automatic renewal policy would enable automatic creation of a new set of credentials using the Dorian certificate authority, whereas a manual renewal policy would require an administrator to do so. The User Policy framework is extensible; administrators can implement local policies.

Each registration authority must also specify its own certificate. When Dorian receives a SAML assertion signed by a registration authority it verifies that the assertion was signed with the private key that corresponds to the registration authority's certificate. Finally, each registration authority must be configured with a list of acceptable authentication methods. A SAML authentication assertion specifies the method in which the credential provider authenticated the user. In order for the SAML assertion to be accepted by Dorian, the authentication method specified in the assertion must be specified as acceptable in the corresponding registration authority.

Account/Certificate Creation

When a user first attempts to create a grid proxy using Dorian, a grid user account is created for them. The account includes user information, user status, user role, and a set of grid credentials including the associated grid identity. The user information includes the user's local institution id, the id of the registration authority the user is associated with, and an email address. The user's status corresponds to the user's current status: Active, Suspended, Pending, or Expired. Only users with an "Active" status may access Dorian. A user's role specifies whether or not the grid user is a Dorian administrator. Only administrators may access the administrative functionality to manage trusted registration authorities or to manage grid accounts. A user's grid credentials consist of a certificate and private key, signed by the Dorian CA that are used by Dorian to issue grid proxy certificates. A user's grid identity is compromised of the Certificate Authority's Subject DN (Distinguished Name), the registration authority Id, and the user's id at his institution. When a user's grid account is created the initial status of the account is "Pending". As mentioned earlier, if the registration authority has an Auto Approval User Policy in place, the status will automatically be changed to "Active", giving the user instant access to Dorian. Administrators can update a user's status and role, and can renew a user credentials.

Grid Proxy Certificate Creation

Users authenticate with grid services using grid proxy certificate (2). Such a grid "proxy" is a short-term credential (private key and certificate) that is created from a user's long-term grid credentials. Dorian facilitates the creation of grid proxies for its users. To create a grid proxy the user supplies a proxy lifetime and the SAML assertion provided by their credential provider to the Dorian client. The Dorian client generates a new public/private key pair and sends the proxy lifetime, public key, and SAML assertion to the Dorian Grid Service. The Dorian Grid Service validates the SAML assertion and employs the user's previously stored grid credentials (long term certificate and private key) to create and sign a proxy certificate for the user-supplied public key. The proxy certificate is then returned to the user. The proxy certificate and locally generated private key can then be used as a grid proxy credential to invoke secure grid services. It is important to note that throughout this process no sensitive information, i.e. private keys, are passed over the network.

Host Certificate Creation

In order to run secure services securely, the container hosting the services must run with a host credential. A host credential consists of a X.509 certificate and private key. The caGrid LOA1 CA/Dorian issues host certificates to users who possess a user certificate issued by the caGrid LOA1 CA. Valid users may request a host certificate from caGrid LOA1 CA/Dorian. To request a host certificate a user must (1) authenticate with caGrid LOA1 CA/Dorian using their grid proxy (2) specify a host name for the certificate, and (3) generate a RSA public/private key pair which will make up the host credentials. From the key pair the public key is sent to caGrid LOA1 CA/Dorian as part of the request, the private key should be securely maintained by the user. All certificate requests require approval of a caGrid LOA1 CA/Dorian administrator. If a caGrid LOA1 CA/Dorian administrator approves the certificate request a host certificate will be created and signed with the caGrid LOA1 CA private key. The host certificate will contain the public key provided by the user and together with the private key securely maintained by the user will make up a host credential. Each host certificate issued by the caGrid LOA1 CA/Dorian is bound to a user or owner, generally the users that requested it; however an administrator may assign a new owner. If the owner's account is revoked, compromised, or suspended any host certificates bound to them will be suspended as well.

Document Name and Identification

Document Title: caGrid LOA1 CA Certificate Policy and Practice Statement

This policy is publish at: https://gforge.nci.nih.gov/frs/?group_id=238

Document Version: 1.0 DRAFT

Document Date: February 21, 2007

OID: 2.16.840.1.113883.3.26.3.2

PKI participants

Certification Authorities

This policy is valid for the caGrid LOA1 CA. The caGrid LOA1 CA will only sign end entity certificates that are intended to identify grid users and grid services. There is no subordinate CA.

Registration Authorities

The caGrid LOA1 CA serves the caBIG™ community. Organizations that are members of the caBIG™ community will serve as Registration Authorities in a manner that their existing vetting and credentialing facilities can be leveraged to integrate with Dorian (1) to allow the caGrid LOA1 CA to issue credentials for their users. Dorian is grid service for the provisioning and management of grid users accounts. Dorian provides an integration point between external security domains and the grid, allowing accounts managed in external domains to be federated and managed in the grid. The CBIIT will evaluate the vetting and credentialing facilities of each member institution and will render a decision on whether or not to allow a member institution to be a Registration Authority (RA). In addition the administrators of the caGrid LOA1 CA will operate a Registration Authority commonly referred to as the Dorian Local Identity Provider (Dorian IdP) which will allow users that are unaffiliated with a caBIG™ member organization to leverage the services of the caGrid LOA1 CA.

Since the caGrid LOA1 CA delegates the identity vetting to organizations with the caBIG™ community, each organization acting as a registration authority to the caGrid LOA1 must be LOA1 certified.

Subscribers

The caGrid LOA1 CA serves the caBIG™ community needs by providing caGrid users and services with X.509 version 3 digital certificates. These certificates may be used for the purpose of authentication, encryption, and digital signing by those individuals to whom the certificates have been issued.

Relying Parties

CBIIT places no restrictions on who may accept certificates it issues.

Other Participants

No Stipulations.

Certificate Usage

Appropriate Certificate Users

One of the purposes of this policy is to promote a wide use of public-key certificates in many different applications. These applications may include, but are not limited to, login authentication, job submission authentication, encrypted e-mail, and SSL/TLS encryption for applications capable of making use of these technologies.

Prohibited Certificate Uses

Other uses of caGrid LOA1 CA issued certificates are not prohibited but are not guaranteed to be supported.

Policy Administration

Organization Administering the Document

The caGrid LOA1 CA is operated by the National Cancer Institute Center for Biomedical Informatics and Information Technology (CBIIT). The CBIIT Compliance Officer is responsible for acceptance of this CPS upon consultation with the CBIIT Director of Core Infrastructure Engineering and the NCI legal advisor to the CBIIT. CBIIT receives policy recommendations from the caGrid Security Working Group, via the caBIG™ General Contractor. The membership of the Security Working Group is available at

http://gforge.nci.nih.gov/frs/download.php/1581/Members-1.0.doc

Contact Person

Contact person for questions related to this document:

Stephen Langella
Ohio State University
333. W 10th Ave.
3190 Graves Hall
Columbus, OH 43210
phone: +1 (614) 292-9845
E-mail: langella@bmi.osu.edu

Contact information regarding other communication with the caGrid Certificate Authority, including security incidents is maintained by CBIIT Application Support at:

ncicb@pop.nci.nih.gov
toll free 1-888-478-4423
toll 301-451-4384

Person Determining CPS Suitability

The National Cancer Institute Center for Biomedical Informatics and Information Technology (CBIIT) will be responsible for determining the suitability of the CPS.

CPS Approval Procedures

This CPS and future revisions of this CPS will require the approval of CBIIT.

Definitions and Acronyms

Certification Authority (CA)
The entity / system that issues X.509 identity certificates (places a subject name and public key in a document and then digitally signs that document using the private key of the CA

Certificate Policy (CP)
A named set of rules that indicates the applicability of a certificate to a particular

community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certification Practice Statement (CPS)

A statement of the practices, which a certification authority employs in issuing certificates.

Certificate Revocation List (CRL)

A CRL is a time stamped list identifying revoked certificates, which is signed by a CA and made freely available in a public repository.

Community RM

One or more RMs that serve multiple, low request rate, sites / Virtual Organizations.

Continuity of Operations Plan (COOP)

A document describing processes and procedures to be followed in the event of a disaster or breach of security when normal operations are not possible.

Distinguished Name DN

An identifier that uniquely represents an object in the X.500 Directory Information Tree (DIT) A DN consists of a set of attribute values that identify the path leading from the base of the DIT to the object that is named. An X.509 public-key certificate or CRL contains a DN that identifies its issuer, and an X.509 attribute certificate contains a DN or other form of name that identifies its subject

Dorian

Dorian is grid service for the provisioning and management of grid users accounts. Dorian provides an integration point between external security domains and the grid, allowing accounts managed in external domains to be federated and managed in the grid.

End Entity

A system entity or person that is the subject of a public-key certificate and that is permitted and able to use, the matching private key only for a purpose or purposes other than signing an X.509 public key certificate; i.e., an entity that is not a CA.

Grid Trust Service (GTS)

The Grid Trust Service (GTS) is a grid-wide mechanism for maintaining and provisioning a federated trust fabric consisting of trusted certificate authorities, such that grid services may make authentication decisions against the most up to date information.

Host Certificate

A Certificate for server certification and encryption of communications (SSL/TSL). It will represent a single machine. Host Certificates are used internally by the PKI service and are not issued to other sites/VOs

Identity Provider (IdP)

An entity that asserts the identity of a user of an electronic information system.

Owner

The human individual or organizational group that has valid rights to exclusive use of a subject name in a certificate. The process of registering the end entity of a certificate request is what maintains the binding between an owner and the subject name (DN).

Person Certificate
A certificate associated with a unique human being.

Policy Management Authority (PMA)
For the caGrid PKI this is a committee composed of the CA managers and representatives from the site/VO Registration Authorities. The PMA has direct responsibility for the CP/CPS and oversight of caGrid operations of the PKI.

Policy Qualifier
The policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

Point of Contact
The member of a site/VO RA that has been chosen to handle all communications about policy matters with the caGrid PMA.

Private RM
RMs that serve high certificate request rate sites / Virtual Organizations, and that are operated by the site/VO.

Registration Authority (RA)
An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).

Registration Agent (RAg) or "Agent"
RAg is the entity that interacts with the RM in order to cause the CA to issue certificates.

Registration Manager (RM)
The RM is the software interface for CA subscribers and agents.

Registered Owner
Once a certificate request has been verified, the ownership of the DN validated, and a certificate issued, the owner is considered to be the "registered owner" of the DN. See above for definition of "Owner".

Relying Party
A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.

Security Incident
An incident that has the potential of private key loss or compromise, regardless of if the compromise or loss was successful. Such incidents include but are not limited to user credential compromise, privilege escalation on systems known to contain private keys, accidental exposure of private keys to unauthorized third parties or loss of a private key.

Service Certificate
A certificate for a particular service running on a host. It will represent a single service on a single host.

Set of provisions
A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS and employing the approach described in this framework.

Subscriber

The person that applied for and was issued a certificate.

Virtual Organization (VO)

An organization that has been created to represent a particular research or development effort independent of the physical sites that the Scientist or Engineers work at. (i.e. PPDG, FNC, EDG, etc).

Publication and Repository Responsibilities

The caGrid LOA1 CA will make its Certificate(s), CP, CPS, CRL and related documents for this CA publicly available. The CA certificate and CRL will be made available through the Grid Trust Service (GTS) (3). The Grid Trust Service (GTS) is a grid-wide mechanism for maintaining and provisioning a federated trust fabric consisting of trusted certificate authorities, such that grid services may make authentication decisions against the most up to date information.

In addition CBIIT will publish the caGrid LOA1 CA CP, CPS, and other related documents to the following website:

https://gforge.nci.nih.gov/frs/?group_id=238

Repositories

The caGrid LOA1 CA repository is maintained by the WSRF-compliant grid service, Dorian running at:

https://cagrid-dorian.nci.nih.gov:8443/wsrf/services/cagrid/Dorian

The caGrid LOA1 CA/Dorian will publish its CA certificate and CRL to the Grid Trust Service (GTS) running at:

https://cagrid-gts-master.nci.nih.gov:8443/wsrf/services/cagrid/GTS

In addition CBIIT will publish the caGrid LOA1 CA CP, CPS, and other related document to the following website:

https://gforge.nci.nih.gov/frs/?group_id=238

Publication of Certification Information

The caGrid LOA1 CA/Dorian operates a secure grid service that contains:

- The caGrid LOA1 CA root self signed certificate and private key.
- All certificates issued by this CA

- The certificate revocation list (CRL) for this CA.

The website maintains:

- All past and current versions of the CP/CPS for this CA and its subsidiaries
- All other published documents related to the caGrid LOA1 CA.

Time and Frequency of Publication

New versions of CP/CPS are published as soon as they have been approved.

The caGrid LOA1 CA/Dorian publishes a CRL immediate following a certificate/account revocation. The CRL will be published to the GTS. The GTS will provision the CRL throughout the entire grid.

Access Controls on Repositories

The CRL, CP, CPS and CA certificate of this CA are made available publically.

The issuance of new certificates, renewal of existing certificates, and the revocation of certificates is only allowed by caGrid LOA1 CA/Dorian administrators and its trusted registration authorities. Trusted registration authorities are only allowed to request Dorian to issue, renew, and revoke certificates for users at or below the security domain for which they are authorized.

Identification and Authentication

Naming

This CA supports multiple registration authorities with different registration processes. In order to become an authorized registration authority, each potential registration authority must have prior approval by CBIIT and must be registered with the Dorian operating the caGrid LOA1 CA as a Trusted Registration Authority. CBIIT ensures that the particular process of the registration authority meets the minimum requirements specified in this CP/CPS.

Using this procedure the RA ensures that:

- It can provide a signed SAML assertion containing the following information for each user in its security (For more details on the SAML Assertions the caGrid LOA1 CA requires consult the following document: http://gforge.nci.nih.gov/plugins/scmcvs/cvsweb.php/cagrid-1-0/Documentation/docs/security/dorian/cabig-dorian-saml-specification.doc?cvsroot=cagrid-1-0):
    - A unique user id within its security domain
    - The first name of the user
    - The last name of the user

    - The email address of the user
- Each RA has been LOA1 certified by CBIIT or by a CBIIT approved organization.

Types of Names

Subject distinguished names (DN) are X.500 names; the caGrid LOA1 CA self signed CA certificate contains the subject:

O=caBIG,OU=caGrid,OU=LOA1,CN=caGrid LOA1 Certificate Authority

The caGrid LOA1 CA issues end entity certificates to users and hosts/services, the distinguished name in each user certificate will consist of the following:

1. The following prefix inherited from the root CA certificate:

   O=caBIG,OU=caGrid,OU=LOA1
2. The name of the Registration Authority (RA) or Identity Provider (IdP) .

   OU=Ohio State University

3. The unique user id assigned to the user by its Registration Authority:

   CN=jdoe

As an example, if the Registration Authority XYZ was been approved by CBIIT and was registered to the caGrid LOA1 CA/Dorian as a trusted Registration Authority, then the distinguished name for the user with the unique user id of jdoe from registration authority XYZ is:

O=caBIG,OU=caGrid,OU=LOA1,OU=XYZ,CN=jdoe

The distinguished name in each host certificate will consist of the following:

1. The following prefix inherited from the root CA certificate:

   O=caBIG,OU=caGrid,OU=LOA1

2. The organization unit “Services” distinguishes that this certificate is intended to identify a host or a set of services.

   OU=Services

3. The name of the host:

   CN= host/myhost.example.com

As an example if the host myhost.example.com were issued a host certificate, the distinguished name would be:

O=caBIG,OU=caGrid,OU=LOA1,OU=Services,CN= host/myhost.example.com

Need for Names to be Meaningful

The Subject and Issuer name contained in a certificate MUST be meaningful in the sense that the RA has proper evidence of the existent association between these names or pseudonyms and the entities to which they belong. To achieve this goal, the use of a name must be authorized by the rightful owner or a legal representative of the rightful owner.

All user certificates issued by the caGrid LOA1 CA contain information such that 1) the registration authority that the user belongs to can be identified and 2) the user can be identified within the registration authority.

All host certificates issued by the caGrid LOA1 CA contain information such that host that the certificate represents can be identified.

Anonymity or Pseudonymity of Subscribers

Anonymity and pseudonymity are not supported.

Rules of Interpreting Various Name Forms

Subject distinguished names are X.500 names; the caGrid LOA1 CA self signed CA certificate contains the subject:

O=caBIG,OU=caGrid,OU=LOA1,CN=caGrid LOA1 Certificate Authority

The caGrid LOA1 CA issues end entity certificates to users and hosts/services, the distinguished name in each user certificate will consist of the following:

4. The following prefix inherited from the root CA certificate:

   O=caBIG,OU=caGrid,OU=LOA1

5. The name of the Registration Authority (RA) or Identity Provider (IdP) .

   OU=Ohio State University

6. The unique user id assigned to the user by its Registration Authority:

   CN=jdoe

As an example if the Registration Authority XYZ has been approved by CBIIT and was registered to the caGrid LOA1 CA/Dorian as a trusted Registration Authority, then the distinguished name for the user with the unique user id of jdoe from registration authority XYZ is:

C O=caBIG,OU=caGrid,OU=LOA1,OU=XYZ,CN=jdoe

The distinguished name in each host certificate will consist of the following:

1. The following prefix inherited from the root CA certificate:

    O=caBIG,OU=caGrid,OU=LOA1

2. The organization unit "Services" distinguishing that this certificate is intended to identify a host or a set of services.

    OU=Services

3. The name of the host:

    CN= host/myhost.example.com

As an example if the host myhost.example.com were issued a host certificate, the distinguished name would be:

O=caBIG,OU=caGrid,OU=LOA1,OU=Services,CN= host/myhost.example.com

Uniqueness of Names

The distinguished names of user certificates issued by the caGrid LOA1 CA are composed of: 1) CA Prefix 2) A unique assigned to the Registration Authority 3) The user's user id within the registration authority. Since each registration authority has a unique id and it is REQUIRED that each registration authority maintains a unique user id for each of its users, the distinguished names issued by the caGrid LOA1 CA are unique.

The distinguished names of host certificates issued by the caGrid LOA1 CA are composed of: 1) CA Prefix 2) the organization unit services 3) The host name of the host the certificate represents. The caGrid LOA1 CA will only issue one certificate per hostname.

Recognition, Authentication, and the Role of Trademarks

No Stipulations.

Initial Identity Validation

The initial registration process with the caGrid LOA1 CA for user certificates consists of the following steps:

1. The requestor requires a grid proxy to access the grid
2. The requestor authenticates to its local credential provider or registration authority using their locally provided credentials.
3. Upon successful authentication, the credential provider / registration authority issues a SAML assertion containing the user's 1) local user id 2) first name 3) last name, and 4) email address.
4. The requestor receives the SAML assertion from the credential provider / registration authority.
5. The requestor generates a public/private key pair to be used for the X.509 proxy certificate.
6. The requestor requests the Dorian operating the caGrid LOA1 CA[1] to create X.509 Proxy certificate. The requestor supplies the SAML Assertion, proxy public key, and the length of time for which the proxy is to be valid.
7. The Dorian operating the caGrid LOA1 CA validates the SAML assertion supplied ensuring that it is signed by a trusted registration authority and that is contains the user's local user id, first name, last name, and email address.
8. If a caGrid account already exists for the user within the Dorian operating the caGrid LOA1 CA, Dorian will proceed to the next step. **Otherwise an account will be created, and the caGrid LOA1 CA Dorian will generate a private key and long term (~1 year) certificate, signed by the caGrid. The user's private key will be wrapped by an RSA key existing in a hardware security module (HSM). The user's certificate and wrapped private key will be stored in a database.**
9. Dorian will create a X.509 proxy certificate based on the public key supplied by the requestor, the X.509 proxy certificate will be signed by the user's long term certificate.
10. Dorian will return the X.509 proxy certificate to the requestor. The requestor now holds a private key (locally generated and held) and a X.509 proxy certificate bound to the locally held private key and signed by the user's long term certificate which is signed by the caGrid LOA1 CA.

The initial registration process with the caGrid LOA1 CA for host certificates consists of the following steps:

1. Obtain caGrid LOA1 CA/Dorian user account.
2. Locally generate an RSA Public/Private key pair.
3. Request a host certificate from Dorian, submitting the Public key generated and the hostname of the host the certificate will represent.
4. On receiving a host certificate request the Dorian operating the caGrid LOA1 CA will require that the requestor authenticate with a X.509 proxy certificate that is rooted by the caGrid LOA1 CA

---

[1] Explanatory comment: Because the caGrid technology (including GAARDS and Dorian) is available for download and reuse by other entities, more than one operating instance of Dorian may exist at any particular time. Data services operating under the aegis of the caGrid LOA1 CA, will require certificates issued by the Dorian service under the control of the caGrid PMA or certificates derived from an external certificate authority with a trust agreement with the caGrid PMA.

certificate. If the authentication is successful, Dorian will ensure that it manages an account for the requestor and that the account is active. If the requestor is an active user Dorian will store the host certificate request for an administrator to review.

5. If an administrator approves the host certificate request a host certificate will be created consisting of the public key provided by the requestor. The host certificate will be signed with the caGrid LOA1 CA private key.
6. Once approved the host certificate may be downloaded by the requestor and together with the generated private key may be used as a host credential.

Method to Prove Possession of Private Key

The caGrid LOA1 CA does not need to do this for a user's long term credentials, since the user's private key is generated and managed by Dorian. Users don't have access to their private key; their private key is used to sign short term X.509 proxy certificates. For host certificates Dorian requires that users authenticate with a X.509 proxy certificate which is signed by the user's private key and is rooted with a the caGrid LOA1 CA certificate which is signed with the caGrid LOA1 CA's private key.

Authentication of Organizational Identity

Each caGrid LOA1 CA registration authority represents an organization. It is required that each organization maintains a local user identity for each user. This local user identity is bound to an account and a person within organization.

Authentication of Individual Identity

Individual user identities will be authenticated through the local organization's/registration authority's identity management system. It is required that that the organization's identity management systems be LOA1 certified.

Non-verified Subscriber Information

Each user's local user id, first name, last name, and email address will be verified against the identity management system of the organization in which the user belongs. No other subscriber information will be verified.

Validation of Authority

Users requesting certificates must first authenticate with the identity management system of the organization in which they belong

Criteria for Interoperation

The caGrid LOA1 CA is intended to interoperate with other CAs in the caBIG™ community.

Identification and Authentication for Re-key Requests

Identification and Authentication for routing Re-Key

caGrid LOA1 CA administrators may request a re-key, administrators must authenticate with the caGrid LOA1 CA/Dorian using an X.509 proxy certificate that identifies them.

For user certificates, the caGrid LOA1 CA/can be configured (per Registration Authority) to automatically perform a re-key when a user's certificate expires. The re-key occurs when the user requests the creation of a proxy certificate, which requires the submission of a SAML assertion signed by the organization's identity management system in which the user belongs. The SAML assertion proves to the caGrid LOA1 CA/Dorian the user's identity. The re-key generates a new certificate and private key, the certificate contains the same Domain Name (DN) as the user's previous certificate and is signed by the caGrid LOA1 CA.

For host certificates only caGrid LOA1 CA/Dorian administrators may perform a re-key.

Identification and Authentication for Re-key After Revocation

If the compromise was limited to just the private key, the request for re-key will be performed by a caGrid LOA1 CA administrator.

If the compromise involved a user's local credentials at their local organization, the user's certificate will be revoked and a re-key will not occur until the local credentials have been re-issued.

Identification and Authentication for Revocation Requests

Only caGrid LOA1 CA administrators may revoke a certificate. Administrators must authenticate with the caGrid LOA1 CA/Dorian using an X.509 proxy certificate that identifies them. Those that are not caGrid LOA1 CA administrators may request to have a certificate revoked by contacting CBIIT.

Certificate Life-Cycle Operational Requirements

Certificate Application

Who can submit a certificate application

Any user who has been issued a user account by an organization operating as a caGrid LOA1 CA Registration Authority may submit an application for a user certificate. Users who are not affiliated with an organization acting as a caGrid LOA1 CA Registration Authority may submit an application to the Dorian Local IdP or the Registration Authority operated by the administrators of the caGrid LOA1 CA. Any user that the caGrid LOA1 CA has issued a user certificate to may request host certificates. Issuance of host certificates requires administrative approval.

Enrollment Process and Responsibilities

Enrollment process used by subscribers and requesters to submit certificate applications:

- The requestor must have a local user account with an organization that is a caGrid LOA1 CA Registration Authority or with the Dorian Local IdP.
- A certificate is requested the first time the user requests an X.509 proxy certificate from the caGrid LOA1 CA. Requesting a X.509 proxy certificate requires (1) authenticating to their local organization; (2) the user to supply SAML assertion proving that the user authenticated to their local organization. The SAML assertion MUST be signed by a caGrid CA Registration Authority.

Subscribers and requesters must:

- Have a basic understanding of the proper use of public key cryptography and certificates;
- Ensure that information provided by their organization's identity management system is accurate.
- Generate a new, secure, and cryptographically sound key pair or have one generated by an appropriate method for each X.509 certificate requested ;
- Read and agree to all terms and conditions of this CP/CPS;
- Use caGrid LOA1 CA issued certificates exclusively for legal and authorized intended purposes;
- U se a caGrid LOA1 CA issued certificate exclusively on behalf of the person, entity, or organization listed as the Subject of such certificate;
- Protect the proxy private key(s) from unauthorized access;
- Protect the host private key(s) from unauthorized access;
- Notify the registration authority of any change to any information included in the certificate or any change in any circumstances that would make the information in the certificate misleading or inaccurate;
- Immediately cease to use the certificate if any information included in the certificate or if any change in any circumstances would make the information in the certificate misleading or inaccurate;
- Protect local account information from un-authorized access.
- Immediately notify the registration authority and cease the use of proxy certificates if their local account credentials (those used in requesting a proxy certificate) have been compromised.
- Use their own judgment about whether it is appropriate, given the level of security and trust provided by a certificate issued by this CA, to use such a certificate in any given circumstance;
- Comply with all laws and regulations applicable to a subscriber's right to export, import, and/or use a certificate issued by this CA and/or related information. Subscribers shall be responsible for procuring all required licenses and permissions or any export, import, and/or use of a certificate issued by this CA and/or related information.

Certificate and Application Processing

Performing Identification and Authentication Functions

The caGrid LOA1 CA identifies all certificate requests by requiring that users authenticate with an organization operating as a caGrid LOA1 CA registration authority. Authentication requires the user to supply credentials to an account operated by the organization's identity management system. The organization's identity management system is REQUIRED to issue and sign a SAML assertion as proof that the user successfully authenticated. The caGrid LOA1 CA will ONLY accept SAML assertion signed by a trusted registration authority as proof of authentication.

Approval or Rejection of Certificate Applications

The caGrid LOA1 CA will approve, reject, or require further investigation of certificate applications based on the following criteria:

1. The user's ability to supply a SAML Assertion signed by a Trusted Registration Authority proving authentication
2. The policy of their registration authority.

Time to Process Certificate Applications

The caGrid LOA1 CA/Dorian will be process certificate application as soon as they are received, applications will immediately be approved or rejected unless it is determined by the policy of the registration authority that further investigation is required.

Certificate Issuance

CA Actions during Certificate Issuance

User Certificates

A certificate request is created for the user the first time the user requests an X.509 proxy certificate from the caGrid LOA1 CA/Dorian. In processing the request the caGrid LOA1 CA first validates that the user supplied an appropriate SAML Assertion, signed by a Trusted Registration Authority. Each registration authority is configured with a policy that is executed and enforced each time a user request an X.509 proxy certificate. This policy contains the business logic for processing certificate requests from users associated with the RA. The outcome of executing this policy on a user's certificate request is either approval of the request, rejection of the request, or no action. If the request is approved a certificate is immediately issued and the user's request for an X.509 proxy certificate is honored as are subsequent requests for a proxy certificate assuming the user's certificate has not been revoked or that subsequent execution of the policy does not revoke the user's certificate. If the request is rejected, the user's request for an X.509 proxy certificate is rejected and will subsequently be rejected. If no action is taken the certificate request will require further investigation by a caGrid LOA1 CA administrator, the user's request for an X.509 proxy certificate is rejected, subsequent requests for proxy certificates will depend on the action taken by the caGrid LOA1 CA administrator.

Host Certificates

Only users that have been issued credentials by the caGrid LOA1 CA may request a host certificate. Upon receiving a host certificate request the caGrid LOA1 CA requires the requestor to authenticate with their caGrid LOA1 CA issued credentials. Upon successfully authenticating the validity of the request is check as follows 1) an active certificate for the host specified in the request does not exist, 2) that a valid public key was submitted with the request and 3) that the public key provided in the request is not the same key used in any compromised certificates. If the request is validated the request is stored to await administrative approval. If the request is approved by an administrator a certificate will be created for the host specified with the public key provided. The host certificate is signed with the caGrid LOA1 CA private key.

Notification to Subscriber by the CA of Issuance of Certificate.

The caGrid LOA1 CA/Dorian does not provide direct notification of certificate issuance. For user certificates since a certificate request is created for the user the first time the user requests an X.509 proxy certificate from the caGrid LOA1 CA/Dorian it can be assumed that a certificate has been issued if a X.509 proxy certificate is issued in result of the user's request. If the certificate request is rejected the use will be informed that their account has been rejected upon requesting a proxy. If further investigation is required, the user will be informed of this when requesting a proxy certificate; in this case it will be up to the caGrid LOA1 CA administrator investigating the request to notify the user whether or not a certificate has been issued.

For host certificates the software enables users to check the status of their host certificate requests. Upon approval it is common (but not required) for administrators to send notification directly to the requestor.

Certificate Acceptance

Conduct Constituting Certificate Acceptance

A certificate request is created for the user the first time the user requests an X.509 proxy certificate from the caGrid LOA1 CA/Dorian. If the certificate request is accepted the caGrid LOA1 CA will honor the user's request and an X.509 proxy certificate will be sent to the user. Since the caGrid LOA1 CA runs as a web service it is assumed that most application will interact with it using a common client API. The following is the process for interaction and acceptance of the x.509 proxy certificate.

1) Authenticate with local organizations and obtains signed SAML assertion.
2) Application/Client API generates public/private key pair for use with X.509 proxy.
3) SAML Assertion, public key, and other metadata submitted to caGrid LOA1 CA in a request for X.509 proxy certificate.
4) If first time requesting a X.509 proxy certificate a request for a long term certificate is generated.
5) If long term certificate request is approved a X.509 proxy certificate is created and signed with the private key associated with the long term certificate. The X.509 proxy certificate is returned to the requestor.
6) The X.509 proxy certificate and locally generated private key is returned to the application or entity leveraging the client API.

For host certificates requests, users may check the status of their host certificate requests. If approved the status of their request will be set to Active and they will be able to download their host certificate.

Publication of the Certificate by the CA

Certificates are not published by the caGrid LOA1 CA.

Notification of Certificate Issuance by the CA to Other Entities

No notification to other entities will be performed.

Key Pair and Certificate Usage

Subscriber Private Key and Certificate Usage

Subscribers must use their certificates appropriately and must:

- Use certificates exclusively for legal and authorized intended purposes;
- Use a certificate exclusively on behalf of the person, entity, or organization listed as the Subject of such a certificate;
- Refrain from using the subscriber's private key corresponding to the public key certificate to sign other certificates, with the exception of proxy certificates as described in RFC 3820.
- Promptly notify the CA operators of any incident involving a possibility of exposure of a private key.

Relying Party Public Key and Certificate Usage

Relying parties shall:

- Be held responsible to understand the proper use of public key cryptography and certificates;
- Read and agree to all terms and conditions of this CP/CPS;

- Verify certificates issued by this CA, including use of CRLs, in accordance with the certification path validation procedure specified in ITU-T Rec. X.509:1997 | ISO/IEC 9594-8 (1997), taking into account any critical extensions, key usage, and approved technical corrigenda as appropriate;
- Trust and make use of a certificate issued by this CA only if such certificate has not expired, been suspended or been revoked and if a proper chain of trust can be established to a trustworthy issuing party;
- Make their own judgment and rely on a certificate issued by this CA only if such reliance is reasonable in the circumstances, including determining whether such reliance is reasonable given the nature of the security and trust provided by a certificate issued by this CA and the value of any transaction that may involve the use of the aforementioned certificates;

Certificate Renewal

The caGrid LOA1 CA/Dorian supports the automatic renewal of user certificates. This feature can be enabled/disabled per Registration Authority. If this feature is enabled a user's certificate will be renewed the next time they request a X.509 proxy certificate after their long term certificate has expired. caGrid LOA1 CA/Dorian administrators may renew a user's certificate at anytime.

At this time host certificate can only be renewed by caGrid LOA1 CA/Dorian administrators.

Certificate Re-Key

Certificates in the caGrid LOA1 CA can be re-keyed by caGrid LOA1 CA/Dorian administrators.

Certificate Modification

Certificates in the caGrid LOA1 CA are not modified.

Certificate Revocation and Suspension

caGrid LOA1 CA issued certificates can be revoked at anytime by caGrid LOA1 CA administrators. In most cases a certificate is revoked for one of the following reasons:

- The private key of the CA or any of its superior CAs has been compromised.
- The private key associated with the certificate is compromised.
- The private key store (= cryptographic token) is lost.
- The certificate subject is no longer valid (ex: name change, employer change)
- The subscriber does not comply with the terms and conditions of this CP/CPS.
- The certificate was not issued in compliance with the terms and conditions of this CP/CPS.

Although ONLY caGrid LOA1 CA administrators may revoke certificates, any person may request that a certificate be revoked. Revocation requests by persons other than caGrid LOA1 CA administrators must be submitted in writing to the caGrid PMA with appropriate justification supporting the proposed revocation.

Facility, Management, and Operational Controls

Physical Controls

Site Location and Construction

The caGrid server is located on one floor of a facility in the Gaithersburg, Maryland area that has two entryways/exits. There is another floor to the building located above the server facility but there is no direct access between the two floors.

Physical Access

Controlled Access. The CaGrid server is located in a facility that maintains the same physical and environmental security controls as are in place for the NCI Network facility. There is a video camera system on site that is monitored by guards at the nearby NCI facility. There is also a proximity card system operated by the National Cancer Institute (NCI) that provides access control to building. NCI Network equipment such as file servers, routers, switches, and other infrastructure peripherals are maintained in a secure sever room.

Access to Sensitive Facilities. Access to the building outside of normal business hours is restricted and controlled through a programmable magnetic card-access system. Access to the computer room itself and other sensitive areas within the building are also controlled by this system.

Use of Keys or Access Devices. A keycard is needed to enter the sever room. The room door remains unmarked

Security of Entry Devices or Keys. Unused hard key are secured in the LAN room. This room requires card key access and all card reader transactions are recorded in the access control program.

Emergency Exit and Re-Entry Procedures. Access to facilities requires a key for sensitive areas or badge pass for general areas thus allowing only authorized personnel to re-enter in the event of an emergency. There are emergency exit and reentry procedures for the. They are enumerated in the building Continuity of Operations Plan .

Visitor Controls. Visitors to server room are signed in. Visitors are authenticated through use of preplanned appointments.

Physical Access Monitoring. The facility owner monitors physical accesses through audit trails, investigates apparent security violations, and takes remedial action. Access to the building outside of normal business hours is restricted and controlled through a programmable magnetic card-access system.

Access to the computer room itself and other sensitive areas within the building are also controlled by this system. The management of the facility handles this process under contract to NCI.

Investigation of Suspicious Activity. The system owner investigates suspicious access activity and takes appropriate action. Any suspicious activity is immediately reported by the ATC to Montgomery County police. The police also routinely patrol the area.

Visitor Authentication. The system owner ensures that visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.

Power and Air Conditioning

Heating and Air-Conditioning System Maintenance. Maintenance of heating and air-conditioning systems is scheduled for all buildings at least twice annually.

Redundant Air-Conditioning System. A redundant air-cooling system is in operation. This system includes an additional back-up fan, which operates independently from the primary fan, and a thermal control circuit that includes a solid-state temperature sensor. This sensor detects ambient temperature changes inside the power supply and is connected to the fan power drives of both the primary and back-up fans. The thermal control circuit works with the temperature sensor to trigger a response whenever specific high and low temperature thresholds are exceeded. This circuitry enables the primary fan to increase its RPM simultaneously with increases in the ambient temperature until reaching full speed.

Power supply fans inevitably break down over long periods of use simply due to their parts wearing out. When this happens or if the ambient temperature is detected as exceeding approximately 68° C, the back-up fan automatically turns on. System administrators have advance warning of fan breakdown or dangerous rises in the power supply temperature. Moreover, the system is protected until it can be safely shut down to replace the primary fan or to correct any unrelated cause of heat problems.

Utility Risk Review. The NIH Office of Research Services (ORS) periodically reviews electric power distribution, heating plants, water, sewage, and other utilities for risk of failure twice per year. The NIH ORS periodically reviews electric power distribution, heating plants, water, sewage, and other utilities for risk of failure. All utility maintenance is handled at the NIH level by ORS.

Water Exposure

Plumbing. Plumbing lines are inspected twice per year. The building plumbing line locations do not endanger the system.

Fire Prevention and Protection

Fire Suppression and Prevention Devices. Appropriate fire suppression and prevention devices are installed and working. All NCI spaces, including the computer and server rooms and wire closets are equipped with a fire detection, notification and suppression system that suppress fire by discharging a gas onto the surface of combusting materials to minimize damage Other environmental safeguards include air conditioning, separate from the main building, for climate control and an Uninterruptible Power Supply (UPS) to facilitate a graceful shutdown of the computer equipment in case of power outage.

The computer room is also integrated with the building power generator. The generator will allow additional time for the graceful shutdown.

Media Storage

Media Control Processes. The system owner has established processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information. All printed material is either stored in file cabinets or is shredded when no longer needed. All electronic media is either stored or overwritten when no longer required.

All media sets (incremental and full) are maintained for 1 year at which time media can be recycled back into the rotation schedule. New tapes are added to the system on a regular schedule; the oldest tapes are removed and stored. Full backups are retrieved from the systems and stored on a regular schedule in a separate storage facility that contains current media. Upon collecting the next set of full backups the following week, the previous week's set are relocated to the archive media locker.

Physical Media Control Processes. The system owner has established processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media. All printers are located in secure areas. Printed documents are printed on printers assigned to each user, who immediately pick up the document upon printing. Electronic access is controlled by "least privilege" assignment of rights. Sensitive printed material is confined to the authorized user's office or work area. Archived storage media is secured by cabinets in a limited access area with limited distribution of keys.

Archived media is currently stored offsite in specialized media cabinets in an environmentally controlled room in a building separate from server rooms and primary/current backup operations/media. The room is secured by lock and key with limited distribution of keys based on need. The room is manned by a property monitor who is responsible for logging the flow of equipment to and from the room.

Media Sanitization. The system owner ensures that media is sanitized for reuse. The NIH Sanitization Policy describes procedures for sanitizing media for reuse.

Disposal of Damaged Media. The system owner ensures that damaged media is stored and /or destroyed. The NIH Sanitization Policy describes procedures for disposal of damaged media.

Once the drives are clean or have been physically damaged, form NIH 2790 (Removal of Data and Software form) is filled out; a copy is attached to the equipment. Form NIH 2790 contains all the information about the hardware (NIH decal #, Man info, Model info, serial #,etc) and notes the working status/condition of the equipment. The Property Office is contacted and the surplus hardware is picked up. The hardware is then sent to a large storage facility where non profit groups can pick up the hardware.

Disposal of Hardcopy Media. The system owner ensures that hardcopy media is shredded or destroyed when no longer needed.

Media is degaussed and sanitized by a contractor as needed. A certificate provided by the contractor is on file at NCI declaring the procedure to be in accordance with the Department of Investigative Service and the Department of Defense procedures.

Water Disposal

In the event of water infiltration there would be a joint coordination between ORS Emergency Preparedness Services, NCI Space and Facilities, Office of Research Services, and/or the landlord. The Facilities Manager for the site is the Occupant Emergency Coordinator and would spearhead the effort.

Off-site Backup

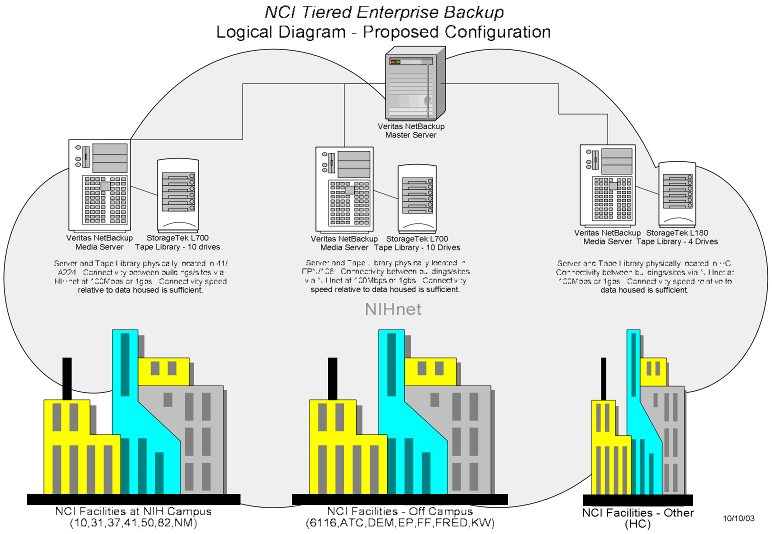
Backup Creation and Rotation. The system owner creates backup files on a prescribed basis that are rotated off-site often enough to avoid disruption if current files are damaged.

NCI currently backs up its servers (NetWare, Windows, UNIX); servers for some groups within NCI; and scientific equipment (which is unable to directly store its data on the server). As a policy, NCI does not backup user workstations. We generally configure workstations to save data in one of two network locations; home drive (H) or group drive (L). There are a few exceptions to this rule.

NCI performs full backups every Friday starting at 10:30 p.m. and running to 7:00 a.m. on Sunday. NCI performs maintenance on the 3rd Saturday of every month. For the Friday preceding the maintenance, a full backup is **NOT** run, but is replaced by and incremental backup. This backup runs on the maintenance Saturday, 12:00 a.m. to 2:00 p.m. This backup is performed in favor of the full backup to ensure that the backups will not interfere with maintenance activities. NCI also performs incremental backups Sunday through Thursday between the hours of 10:30 p.m. and 7:00 a.m.

A full backup copies all files and folders on the target system to tape cartridge. An incremental backup copies all files and folders that have changed since the last successful full or incremental backup.

NCI employs Veritas NetBackup version 5.1, maintenance pack 6. NetBackup employs a tiered strategy to enterprise backup. The following diagram depicts the NCI implementation of this tiered strategy:


NCI Tiered Enterprise Backup
Logical Diagram - Proposed Configuration
Veritas NetBackup Master Server
Veritas NetBackup Media Server
StorageTek L700 Tape Library - 10 drives
Server and Tape Library physically located in 41/A224. Connectivity between buildings/sites via NIHnet at 100Mbps or 1gbs. Connectivity speed relative to data housed is sufficient.
Veritas NetBackup Media Server
StorageTek L700 Tape Library - 10 Drives
Server and Tape Library physically located in EPN/108. Connectivity between buildings/sites via NIHnet at 100Mbps or 1gbs. Connectivity speed relative to data housed is sufficient.
Veritas NetBackup Media Server
StorageTek L180 Tape Library - 4 Drives
Server and Tape Library physically located in HC. Connectivity between buildings/sites via NIHnet at 100Mbps or 1gbs. Connectivity speed relative to data housed is sufficient.
NIHnet
NCI Facilities at NIH Campus (10,31,37,41,50,82,NM)
NCI Facilities - Off Campus (6116,ATC,DEM,EP,FF,FRED,KW)
NCI Facilities - Other (HC)
10/10/03

Procedural Controls

All persons with access to the systems hosting the caGrid LOA1 CA will be NCI CBIIT approved personnel. Personnel will be NCI CBIIT Operations staff, NCI CBIIT Security Operations staff, and NCI CBIIT System administration staff. Dorian software developers do not have direct access to the production Dorian instance.

Personnel Controls

Operators of the caGrid LOA1 CA will be qualified system administrators and operators at NCI CBIIT.

Audit Logging Procedures

Types of Events Recorded

No Stipulation.

Frequency of Processing Log

No Stipulation.

Retention Period for Audit Log
No Stipulation.

Protection of Audit Log
No Stipulation.

Audit Log Backup Procedures
No Stipulation.

Audit Collection System (internal vs external)
No Stipulation.

Notification of event-causing subject
No Stipulation.

Vulnerability Assessments
No Stipulation.

Records Archival
No Stipulation.

Key Changeover
Best effort will be made to notify relying parties of any new public key for the caGrid LOA1 CA. In event of a key change over the new root certificate will be published immediately to the Grid Trust Service (GTS).

Compromise and Disaster Recovery

Incident and Compromise Handling Procedures

All incidents will be-handled by CBIIT in accord with established NCI procedures and in accord with the NCI and NIH COOP plans.

Computing Resources, Software, and/or Data are Corrupted

All incidents will be-handled by CBIIT in accord with established NCI procedures and in accord with the NCI and NIH COOP plans.

Entity Private Key Compromise and Procedures

Any private key compromises will be handled by CBIIT on a case-by-case basis. In general an attempt will be made to identify any affected parties and notify those parties. If a user or host certificate private key is compromised the following actions will be taken:

- The certificate associated with the private key will be revoked and added to the CRL.
- Pending an investigation a new key pair and certificate will be created.

If the private key that a registration authority uses to sign SAML assertions is suspected to be compromised, the following actions will be taken:

- Registration Authority will immediately be removed as a Trusted Registration Authority
- All accounts associated with the registration authority will be suspended.
- All certificates issued by the caGrid LOA1 CA that are associated with the compromised Registration Authority will be revoked.
- A CRL containing the list of revoked certificates will be published to the Grid Trust Service (GTS).

After an investigation into the compromise situation has been performed and the registration authority has been evaluated by CBIIT, if the registration authority is reinstated, it will be required to obtain a new private key and certificate for signing SAML assertions in order to be re-admitted as a trust registration authority. Once the registration authority is re-admitted, the caGrid LOA1 CA/Dorian will be configured to only accept SAML assertions signed with the new key, user's with certificates issued under the re-admitted registration authority will be granted access again.

If the private key of the caGrid LOA1 CA is suspected to be compromised, CBIIT must be informed immediately. The following steps will be taken:

- Revoke the CA certificate
- Immediately suspend the CA from the Grid Trust Service (GTS)
- Immediately terminate the Dorian instance operating the caGrid LOA1 CA.
- Notify all subscribers with certificates issued by the CA on a best effort basis
- Revoke all subscriber certificates and issue new CRLs.
- Determine the cause of the key compromise and correct the situation
- Replace all newly revoked certificates
- The revoked CA will generate a new key pair and self-signed certificate.

- The new CA certificate will be published to the Grid Trust Service (GTS)
- Issue new CRL's

Business Continuity Capabilities after a Disaster

In the case of a disaster whereby the caGrid LOA1 CA installation is physically damaged and all copies of the CA signature keys are destroyed as a result, CBIIT will take whatever action is deemed appropriate at the time based on current CBIIT continuity of operations plans (COOP).

CA or RA Termination

If the NCI caGrid LOA1 CA ceases operation, all the certificates issued by that CA will be revoked immediately and the CA will be removed from the Grid Trust Service (GTS).

Technical Security Controls

Key Pair Generation and Installation

Key Pair Generation

The caGrid LOA1 CA/Dorian maintains a CA private key and certificate for each of its users. All private keys are wrapped with a key stored in a Hardware Security Module (HSM). A user's certificate and wrapped private key are stored in a local database.

The caGrid LOA1 CA/Dorian does not generate or maintain private keys for host certificates. Private keys for host certificates are generally generated by client side software.

The caGrid LOA1 CA/Dorian does not generate or maintain private keys for X.509 proxy certificates. Proxy private keys are generally generated by client side software.

Private Key Delivery to Subscriber

Users' long term private keys are NEVER delivered to subscribers; instead they are used to sign X.509 proxy certificates or short term certificates. The private keys associated with the X.509 proxy certificates are generated locally by client side software and thus do not need to be delivered to the subscriber.

Host certificate private keys are generated locally by the requestor of the host certificate and therefore do not need to be delivered.

Public Key Delivery to Subscriber

Public keys for the user's X.509 proxy certificate and long term certificate (associated with the proxy certificate chain) are delivered over an encrypted channel (https).

Public keys for host certificates are delivered over an encrypted channel (https).

CA Public Key Delivery to Relying Parties

The CA public key is distributed to relying parties over an encrypted channel (https) via the Grid Trust Service (GTS)

Key Sizes

The CA private key will be 2048 bits in length. Subscriber private keys will be 1024 bits in length.

Public Key Parameters Generation and Quality Checking

No Stipulation.

Key Usage Purposes (as per X.509 v3 key usage field)

The signing key of this CA is permitted for signing certificates and CRLs and have the Digital Signature, keyCertSign and CRLSign key usage bits set.

Subscriber or user certificates will have the following key usage bits included:

- Digital Signature
- Key Encipherment
- Data Encipherment
- Non Repudiation

Private Key Protection and Cryptographic Module Engineering Controls

Cryptographic Module Standards and Controls

The caGrid LOA1 CA will use a FIPS140-2 level 3 Hardware Security Module for the generation of and storage of its private key. The caGrid LOA1 CA also maintains a 256 bit RSA key (herein referred to as the "Wrapping Key" for wrapping user private keys. The "Wrapping Key" is generated and stored in a FIPS140-2 level 3 Hardware Security Module.

Private Key (n out of m) Multi-Person Control

Not supported.

Private Key Escrow

Not supported.

Private Key Backup

The caGrid LOA1 CA's private key and "Wrapping Key" are backed up across two smartcards, both smartcards are required to restore the keys to the caGrid LOA1 CA's FIPS140-2 level 3 Hardware Security Module.

Private Key Archival

The caGrid LOA1 CA private key will not be archived

Private Key Transfer into or from a Cryptographic Module

Both the caGrid LOA1 CA private key and "Wrapping Key" will be initially generated on the HSM. If for some reason the key needs to be transferred back to the HSM or to another HSM because of unforeseeable problems. The key will be transferred from backups maintained across multiple smart cards.

Private Key Storage on Cryptographic Module

The caGrid LOA1 CA private key are stored on a cryptographic module meeting FIPS 140-2 level 3

Method of Activating Private Key

The private key is activated automatically at server startup to allow immediate caGrid LOA1 CA operation.

Method of Deactivating Private Key

HSM utilities on the server support deactivating the private key.

Method of Destroying Private Key

The HSM Security Officer can reinitialize the HSM to destroy the private key.

Cryptographic Module Rating

The hardware security module meets FIPS140-2 level 3.

Other Aspects of Key Pair Management

Public Key Archival

No stipulation.

Certificate Operational Periods and Key Pair Usage

The caGrid LOA1 CA root certificate will have validity for 10 years.

User certificates issued by the caGrid LOA1 CA will have a validity of 1 year.

X.509 proxy certificates issued by the caGrid LOA1 CA/Dorian will have a maximum validity of 12 hours.

Activation Data

No Stipulation.

Computer Security Controls

The CA Servers are protected by external firewalls that filter all traffic except the essential. Additionally the CA systems themselves are hardened and have a high security operating system installed. Access to the system for system administrators is granted only over secure and restricted protocols using public key authentication.

Specific Computer Security Technical Requirements

No Stipulation.

Computer Security Rating

No Stipulation.

Life-Cycle Technical Controls

No Stipulation.

Network Security Controls

Network security is ensured using firewalls, virus scanners and intrusion detection systems.

Time-Stamping

No Stipulation.

Certificate, CRL, and OCSP Profiles

Certificate Profile

End-entity certificates will be in X509 v3, compliant with RFC 3280.

Version Number(s)

Version of X.509 certificates: version 3

Certificate Extensions

For the CA certificate:

• Key Usage (critical): Digital Signature, Certificate Sign, CRL Sign

• basicConstraints (critical): CA: true, Path Length 1

• X509 V3 SubjectKeyIdentifier

• X509 V3 AuthorityKeyIdentifier

For the User /Host/Service Certificates:

Key Usage(critical): Digital Signature, Key Encipherment, Data Encipherment, Non Repudiation

BasicConstraints(critical): CA:false

X509 V3 SubjectKeyIdentifier

X509 C3 AuthorityKeyIdentifier

Algorithm Object Identifiers

The algorithms with OIDs supported by this CA:

- Algorithm --- Object Identifier
- Sha1WithRSAEncryption --- 1.2.840.113549.1.1.5
- Md5WithRSAEncryption --- 1.2.840.113549.1.1.4
- rsaEncryption --- 1.2.840.113549.1.1.1

Name Forms

User Certificates

All user certificates signed by the caGrid LOA1 CA will have the following name form:

O=caBIG,OU=caGrid,OU=LOA1,OU=**IDP_NAME**,CN=**USER_ID**

Where:

IDP_NAME is the name of the Registration Authority responsible for vetting the identity of the user.

USER_ID is the user's local user identifier at the Registration Authority or within their organization's identity management system.

Host Certificates

All host certificates signed by the caGrid LOA1 CA will have the following name form:

O=caBIG,OU=caGrid,OU=LOA1,OU=Services,CN=host/**HOSTNAME**

Where:

HOSTNAME is the name of the host the certificate represents

Name Constraints

All certificates issued by the caGrid LOA1 CA will have names with the following prefix:

"O=caBIG,OU=caGrid,OU=LOA1"

Certificate Policy Identifier

OID: 2.16.840.1.113883.3.26.3.2

Usage of Policy Constraints Extension

No Stipulation.

Policy Qualifiers Syntax and Semantics

No Stipulation.

Processing Semantics for the Critical Certificate Policy Extension

No Stipulation.

CRL Profile

This CA issues X.509 Version 2 CRLs in accordance with IETF PKIX RFC 3280.

Version Numbers(s)

The CRL version is set to v2.

CRL and CRL Entry Extensions

Version 2 CRL, and CRL extensions and their current status are specified below:

- CRLNumber: Populated by the CA application
- reasonCode: Populated by the CA application as specified by operator. May contain

(0) Unspecified, (1) Key compromise, (3) Affiliation change, (4) Superseded, (5)

Cessation of operation

- authorityKeyIdentifier: Populated by CA application contains key id (SHA1) of issuer public key

OCSP Profile

This CA currently does not support the Online Certificate Status Protocol (OCSP).

Compliance Audit and Other Assessments

Organization will be allowed to audit the caGrid LOA1 CA at the discretion of CBIIT to verify compliance with the rules and procedures specified in this document.

Other Business and Legal Matters

Fees

The caGrid LOA1 CA will charge no fees as such no refunds will be given.

Financial responsibility

The caGrid LOA1 CA accepts no financial responsibility.

Confidentiality of Business Information

The caBIG User CA collects contact information on its subscribers. Some of this information is used to construct unique, meaningful subject names in the issued certificates. Information included in issued certificates and CRLs is **not** considered confidential. The caBIG User CA does not collect any confidential information.

Intellectual Property Rights

The caGrid LOA1 CA asserts no ownership rights in certificates issued to subscribers, but does retain the right to revoke certificates as the PMA may deem necessary.

Acknowledgment is hereby given to the NCSA PKI, the DOE Science Grid and to the Swiss Education & Research Network (SWTICH) for inspiration of parts of this document.

Representations and Warranties

The caGrid CA is operated with a reasonable level of security, but is provided on a best efforts only basis. The U.S. Government, NIH, NCI and their contractors make no warranty, express or implied, including the warranties of merchantability and fitness for a particular purpose with respect to the security or suitability of a service that is identified by a caGrid issued certificate. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government, NIH, NCI or any of their employees or contractors.

Disclaimers of Warranties

No Stipulation.

Limitations of Liability

No Stipulation.

Indemnification

No indemnification of any sort will be provided by the U.S. Government. NIH or NCI.

Term and Termination

Term

This policy is effective immediately after being approved by CBIIT.

Termination

This policy may be terminated at any time without advance notice as needed to protect the infrastructure and or its users, or any affiliated networks..

Effect of Termination and Survival

No Stipulation.

Individual Notices and Communications with Participants

No Stipulation.

Amendments

Procedure for Amendment

Changes to this document may be submitted through the Security Working Group at (insert url here of SWG site or GForge site).

Notification Mechanism and Period

Best effort notification of all relying parties will be made with as much advance notice as possible via the SWG pages on GForge at (insert url here) .

Circumstances Under the OID Must be Changed

Any substantial change of policy will incur a change of OID.

Dispute Resolution Provisions

CBIIT will resolve all disputes regarding this policy.

Governing Law

Interpretation of this policy shall be in governed and in accordance with Federal Statutes, and Regulations of the United States of America as interpreted by the Federal Courts in the District of Columbia and the applicable implementing guidelines issued by Federal Agencies.

Compliance and Applicable Law

No Stipulation.

Miscellaneous Provisions

No Stipulation.

Other Provisions

No Stipulation.

Document Source

This source for this document can be found in the CVS repository managed by the NCICBIT GForge. The CVS repository can be browsed via the web from the following URL:

http://gforge.nci.nih.gov/plugins/scmcvs/cvsweb.php/gridsecurity/?cvsroot=gridsecurity

Works Cited

1. *Dorian: Grid Service Infrastructure for Identity Management and Federation.* **Stephen Langella, Scott Oster, Shannon Hastings, Frank Siebenlist, Tahsin Kurc, Joel Saltz.** Salt Lake City, Utah : The 19th IEEE Symposium on Computer-Based Medical Systems, 2006.

2. *Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile.* **S. Tuecke, V. Welch, D. Engert, L. Pearlman, M. Thompson.**

3. *Enabling the Provisioning and Management of a Federated Grid Trust Fabric.* **Stephen Langella, Scott Oster, Shannon Hastings, Frank Siebenlist, Tahsin Kurc, Joel Saltz.** Gaithersburg : 6th Annual PKI R&D Workshop, 2007.